#11

DECLARATION

I, Manami Enomoto, a staff member of TAIYO, NAKAJIMA & KATO, Seventh Floor, HK-Shinjuku Bldg., 3-17, Shinjuku 4- chome, Shinjuku-ku, Tokyo 160-0022, Japan, do hereby declare that I am well acquainted with the English and Japanese languages and I hereby certify that, to the best of my knowledge and belief, the following is a true and correct translation made by me into the English language of the documents in respect of Japanese Patent Application No. 9-19412 that was filed on 31st January 1997 in the name of TOYOTA JIDOSHA KABUSHIKI KAISHA.

Dated this 20th day of January, 2003

M. Enomoto

Manami Enomoto

[DOCUMENT NAME]	Application for Patent
[REFERENCE NUMBER]	TYP-97033
[FILING DATE]	31st January 1997
[CONSIGNEE]	The Director General of the Patent Office
[I. P. C.]	G08G 1/00 G07B 15/00
[TITLE OF THE INVENTION]	VEHICLE-MOUNTED COMMUNICATION DEVICE AND ROAD-TO-VEHICLE COMMUNICATION DEVICE
[NUMBER OF CLAIMS]	7
[INVENTOR]	
[ADDRESS OR RESIDENCE]	c/o TOYOTA JIDOSHA KABUSHIKI KAISHA of 1, Toyota-cho, Toyota-shi Aichi-ken
[NAME]	Kazumasa Nakamura
[APPLICANT]	
[I. D. NUMBER]	000003207
[NAME]	TOYOTA JIDOSHA KABUSHIKI KAISHA
[REPRESENTATIVE]	Akihiro Wada
[AGENT]	
[I. D. NUMBER]	100079049
[ATTORNEY]	
[NAME]	Jun Nakajima
[TELEPHONE NUMBER]	03-3357-5171
[APPOINTED AGENT]	
[I. D. NUMBER]	100084995
[ATTORNEY]	
[NAME]	Kazuyoshi Kato
[TELEPHONE NUMBER]	03-3357-5171
[APPOINTED AGENT]	
[I. D. NUMBER]	100085279
[ATTORNEY]	
[NAME]	Katsuichi Nishimoto
[TELEPHONE NUMBER]	03-3357-5171
[APPOINTED AGENT]	
[I. D. NUMBER]	100099025
[ATTORNEY]	
[NAME]	Koji Fukuda
[TELEPHONE NUMBER]	03-3357-5171
[APPOINTED AGENT]	
[I. D. NUMBER]	100101269

[ATTORNEY]

[NAME]	Michio Iizuka	
[TELEPHONE NUMBER]	03-3357-5171	
[INDICATION OF FEE]		
[I. D. NUMBER IN ADVANCE PAYMENT REGISTER]		006839
[AMOUNT OF FEE]	21000	
[LIST OF FILED DOCUMENT]		
[DOCUMENT]	Specification	1
[DOCUMENT]	Drawings	1
[DOCUMENT]	Abstract of the Disclosure	1
[GENERAL POWER OF ATTORNEY NUMBER]		9502364

[DOCUMENT NAME] SPECIFICATION

[TITLE OF THE INVENTION]

VEHICLE-MOUNTED COMMUNICATION DEVICE AND ROAD-TO-VEHICLE COMMUNICATION DEVICE

[CLAIMS]

[Claim 1] A vehicle-mounted communication device comprising:

transmitting/receiving means provided for communication of information with road-side communication means located at a road side; and

relay means for relaying encryption information received from the road side by said transmitting/receiving means to an IC card which includes storage means for storing user information regarding a balance of charges and which also includes encryption means that encrypts and outputs output information based on the user information and decodes encrypted input information regarding the user information.

[Claim 2] A vehicle-mounted communication device according to claim 1, wherein said relay means relays the output information encrypted by the IC card to said transmitting/receiving means.

[Claim 3] A vehicle-mounted communication device according to claim 1 or claim 2, further comprising encryption information storage means in which the encryption information is temporarily stored, wherein said transmitting/receiving means stores the encryption information in said encryption information storage means and transmits as is the encryption information stored in said encryption information storage means.

[Claim 4] A vehicle-mounted communication device according to any one of claims 1 to 3, wherein at least one of the IC card and the road-side communication means outputs a portion of the output information in a state without encryption and information display means for displaying the portion of the output information outputted without being encrypted is further provided.

[Claim 5] A road-to-vehicle communication device comprising:

a vehicle-mounted communication device according to any one of claims 1 to 4; and

road-side control means being located at a road side, including road-side communication means provided for intercommunication of information with the vehicle-mounted communication device, and also including

road-side encryption means for encrypting transmitted information and decoding received information.

[Claim 6] A road-to-vehicle communication device according to claim 5, wherein road-side encryption means of said road-side control means installed at an entrance gate effects encryption of transmitted information and road-side encryption means of said road-side control means installed at a toll reception gate effects only decoding of received information.

[Claim 7] A road-to-vehicle communication device according to claim 5 or claim 6, wherein the transmitted information is accounting information regarding accounting processing of charged facilities.

[DETAILED DESCRIPTION OF THE INVENTION]

[0001]

[Technical Field of the Invention]

The present invention relates to a vehicle-mounted communication device and a road-to-vehicle communication device, and particularly to a vehicle-mounted communication device mounted on a vehicle and to a road-to-vehicle communication device which effects communication processing between the vehicle-mounted

communication device and an on-road apparatus installed on a road side.

[0002]

[Prior Art]

In recent years, an automatic toll collecting system has been developed which utilizes a toll pre-paid type card or a toll post-payment type card to receive charges for using charged facilities, for example, to receive a toll charged on a toll road. In the automatic toll collecting system, on-road apparatuses with antennas, each of which serves as an interrogator for making inquiries with respect to a vehicle for information in order to collect tolls automatically at entrance and exit gates of the toll road, are provided on the road side, and each of vehicle-mounted apparatuses for road-to-vehicle communications (hereinafter referred to as "vehicle-mounted apparatuses") with antennas, each of which serves as a responder for responding to the information, with respect to which an inquiry was made is mounted on the vehicle, whereby the information is transferred by radio communications between the vehicle-mounted apparatus and the on-road apparatus.

[0003]

As described above, in order to collect a toll automatically by transferring information between the vehicle-mounted apparatus and the on-road apparatus, vehicle information about a vehicle and user information about a user, such as a balance of charges for accounting must be stored. Accordingly, the IC card in which a large quantity of data can be stored may be used with information being written therein.

[0004]

However, in a case of transferring the above-described information, when the information is used in a general description form, there exists a problem that a person that is not intended by a user or an information provider can illegally alter or falsify the contents of the information and can also unlawfully utilize such information.

[0005]

Accordingly, there has been proposed an automatic toll collecting system in which information communicated between an on-road apparatus and a vehicle-mounted apparatus is encoded so as to improve the security (see Japanese Patent Application Laid-Open (JP-A) No. 6-60237). In this system, encoded information stored in an

IC card or encoded information from the on-road apparatus is made into a common sentence structure (made into a general descriptive form) in the vehicle-mounted apparatus, and processing for user information such as a balance of charges is effected.

[0006]

[Problems to be Solved by the Invention]

However, in the conventional automatic toll collecting system, the user information made into a common sentence structure in the vehicle-mounted apparatus is temporarily stored. Accordingly, a person that is not intended by the user or the information provider can easily falsify the contents of the user information about a user such as the balance of charges, and the like, thereby resulting in deterioration of security.

[0007]

In view of the above-described circumstances, an object of the present invention is to provide a vehicle-mounted communication device and a road-to-vehicle communication device that can allow communication of information using a simple structure by making it difficult to leak or falsify information.

[0008]

[Means for Solving the Problems]

In order to achieve the above-described objects, a vehicle-mounted communication device comprises: transmitting/receiving means provided for communication of information with road-side communication means located at a road side; and relay means for relaying encryption information received from the road side by the transmitting/receiving means to an IC card which includes storage means for storing user information regarding a balance of charges and which also includes encryption means encrypts and outputs output information based on the user information and decodes encrypted input information regarding the user information.

[0009]

The invention of claim 2 is a vehicle-mounted communication device according to claim 1, wherein the relay means relays the output information encrypted by the IC card to the transmitting/receiving means.

[0010]

The invention of claim 3 is a vehicle-mounted communication device according to claim 1 or claim 2, further comprising encryption information storage means

in which the encryption information is temporarily stored, wherein the transmitting/receiving means stores the encryption information in the encryption information storage means and transmits as is the encryption information stored in the encryption information storage means.

[0011]

The invention of claim 4 is a vehicle-mounted communication device according to any one of claims 1 to 3, wherein at least one of the IC card and the road-side communication means outputs a portion of the output information in a state without encryption and information display means for displaying the portion of the output information outputted without being encrypted is further provided.

[0012]

The invention of claim 5 is a road-to-vehicle communication device comprising: a vehicle-mounted communication device according to any one of claims 1 to 4; and road-side control means being located at a road side, including road-side communication means and provided for intercommunication of information with the vehicle-mounted communication device, and also including

road-side encryption means for encrypting transmitted information and decoding received information.

[0013]

The invention of claim 6 is a road-to-vehicle communication device according to claim 5, wherein road-side encryption means of the road-side control means installed at an entrance gate effects encryption of transmitted information and road-side encryption means of the road-side control means installed at a toll reception gate effects only decoding of received information.

[0014]

The invention of claim 7 is a road-to-vehicle communication device according to claim 5 or claim 6, wherein the transmitted information is accounting information regarding accounting processing of charged facilities.

[0015]

At the vehicle-mounted communication device of the invention of claim 1 intercommunication of information is carried out with respect to the road-side communication means located at the road said, with the

transmitting/receiving means. The IC card is attachable and detachable at the vehicle-mounted communication device and stores in the storage means the user information regarding the balance of charges. The encryption means encrypts output information based on the user information and then outputs. The encryption means also decodes the encrypted input information regarding the user information. Among the information received from the road side by the transmitting/receiving means, the encryption information is relayed to the IC card by the relay means. Accordingly, the encryption information passes through the vehicle-mounted communication device in a form of being left unchanged, and thus, the secrecy of the encryption information is maintained and the security thereof is protected.

[0016]

As described in claim 2, the above-described relay means relays the output information encrypted by the IC card to the transmitting/receiving means, so as to transmit the output information based on the encrypted user information from the IC card to the road said in a form of being left unchanged. As a result, the secrecy of the output information can be maintained and the security thereof can be protected.

[0017]

As described in claim 3, the vehicle-mounted communication device can further include the encryption information storage means in which encryption information is temporarily stored. The encryption information storage means stores therein encryption information with the transmitting/receiving means. Further, the stored encryption information is transmitted as is by the transmitting/receiving means. As a result, the encryption information from the road said, which is unrelated to the user information stored in the IC card and is desired to be retained, for example, gate information which indicates an entrance gate, a mid-route, and the like, can be held in a form of being left unchanged and can also be transmitted to the road side. Accordingly, the secrecy of the information from the road side can be maintained and the security thereof can be protected.

[0018]

Further, as described in claim 4, the information display means is further provided which outputs the portion of output information desired to be made known to a user without encryption by the IC card and displays the portion of the output information outputted without being

encrypted, thereby resulting in that the user can confirm completion of communication or details that are results of accounting processing.

[0019]

As described in claim 5, in the road-to-vehicle communication device of the present invention, the IC card is mounted in the vehicle-mounted communication device and information is mutually communicated with respect to the road-side control means located at the road side. The road-side encryption means of the road-side control means encrypts transmitted information and decodes received information. Accordingly, transmitted information to be transmitted from the road side passes through the vehicle-mounted communication device in a form of being encrypted. As described in claim 7 as well, processing such as reception of charges can be effected for the IC card in such a manner that accounting information regarding accounting processing of charged facilities is transmitted and received as the transmitted information, and the resulting information also passes through the vehicle-mounted communication device in the form of being encrypted, thereby resulting in no damage to the secrecy of the information.

[0020]

As described in claim 6, the road-to-vehicle communication device encrypts transmitted information with the road-side encryption means of the road-side control means located at an entrance gate and decodes received information by the road-side encryption means of the road-side control means located at a toll reception gate. As a result, the vehicle-mounted communication device does not have encryption means, and therefore, irregularities in charge payment caused by analysis of a cipher of the vehicle-mounted communication device can be made impossible.

[0021]

[Embodiments]

Embodiments of the present invention will hereinafter be described in detail with reference to the accompanying drawings. The present embodiments each show that the present invention is applied to an automatic toll receiving system for automatically receiving a toll from each of vehicles running on a toll road or the like.

[0022]

In the automatic toll receiving system, information is transferred between an apparatus mounted

on a vehicle and an on-road apparatus having flat antennas (or other antennas, for example, Yagi antennas) provided at ground portions of an entrance gate, an exit gate, and the like through radio communications to thereby determine a traffic section (route) over which the vehicle has been driven and the type of the vehicle and automatically accept a traffic toll or the like without stopping the vehicle at the entrance and exit gates.

[0023]

As shown in Fig. 1, an automatic toll receiving system of the present embodiment is structured to include an on-road apparatus 10 provided on the road side and a vehicle-mounted apparatus 30 mounted on a vehicle, and information is mutually transferred between the on-road apparatus 10 and the vehicle-mounted apparatus 30 by radio communications. The on-road apparatus communicating with the vehicle-mounted apparatus 30 is provided with flat antennas (or other antennas, for example, Yagi antennas) for transmitting and receiving various information and is disposed at each of an entrance gate of a toll road, a mid-route (check barrier), and an exit gate or the like. The on-road apparatus 10 includes a memory 28 (see Fig. 4) in which an electronic key I for encryption of information is stored and the vehicle-

mounted apparatus 30 includes a storage circuit 48 (see Fig. 3) in which the above-described encryption information is stored, as will be described in detail later. When information is mutually transferred between the on-road apparatus 10 and the vehicle-mounted apparatus 30 by radio communications, transmitted information is encrypted using the electronic key I on the side of the on-road apparatus and is transmitted to the vehicle-mounted apparatus 30. This encryption (or decoding) can be provided using a method based on Data Encryption Standard (a so-called DES) or the like.

[0024]

An IC card 62 (which will be described in detail later) in which various information is stored is provided so as to be detachable from the vehicle-mounted apparatus 30. Information is mutually transferred between the vehicle-mounted apparatus 30 and the IC card 62. The IC card 62 includes a memory 70 (see Fig. 5) in which a security mechanism A provided with a process for encrypting or decoding information is stored. This security mechanism is used to manufacture or issue the IC card 62 and is in advance set in accordance with an operation thereof. A plurality of logic which are provided for encryption or decoding by the security

mechanism can be stored on the side of the on-road apparatus and any one security mechanism can be selectively used.

[0025]

Next, the vehicle-mounted apparatus 30 and the on-road apparatus 10 communicating with the vehicle-mounted apparatus 30 will be described in detail. Further, in the present embodiment, a description will be given in which an on-road apparatus provided in the mid-route 200 is shown as an example. Further, for simplifying an explanation, a mid-route antenna 218 provided for radio communication with a vehicle 90 traveling along a lane 202 and a mid-route antenna control device 232 are used for the explanation. Further, a vehicle-mounted battery (not shown) is connected to the vehicle-mounted apparatus 30.

[0026]

As shown in Fig. 2, in the mid-route 200 located immediately before or after a branching point of a toll road, two lanes, the lane 202 and a lane 204, are provided side by side between a ground 208 and a ground 214. An arch 216 is disposed between the ground 208 and the ground 214 in such a manner as to extend over the lanes 202 and

204. Route recognizing antennas 218, 220, and 222 are disposed on the arch 216. The route recognizing antenna 218 is located above the lane 202 for radio communication with a vehicle traveling along the lane 202. The route recognizing antenna 222 is located above the lane 204 for radio communication with a vehicle traveling along the lane 204. The route recognizing antenna 220 is disposed substantially at an intermediate point between the route recognizing antennas 218 and 222 such that it is located above a centerline 206 between the lanes 202 and 204, for radio communication with a vehicle running so as to straddle the boundary between the lanes 202 and 204.

[0027]

A route control center 230 equipped with the route recognizing antenna control device 232 is disposed on the ground 214. The route recognizing antennas 218, 220, and 222 are connected to the route recognizing antenna control device 232.

[0028]

In the above-described mid-route 200, the route recognizing antenna control device 232 transmits route information, which represents the kind of route a vehicle 90 traveled on a toll road, to the vehicle-mounted device

30 mounted on the vehicle 90, via the route recognizing antenna. The route recognizing antenna control device 232 can be connected to a central computer for collectively controlling a running state of the vehicle on the toll road. A recovery gate can be disposed at the mid-route 200 so as to write the route information indicating a mid-route into the vehicle-mounted apparatus using the IC card 62. The recovery gate is provided with an IC card read/write device in which the IC card 62 is removably mounted. The IC card read/write device is connected to the central computer. The recovery gate may be disposed at a parking area or a service area.

[0029]

Meanwhile, at the entrance gate that is another on-road apparatus, entrance information of the toll road is transmitted to the vehicle-mounted apparatus 30 mounted on the vehicle. Further, at the exit gate, exit information which indicates an exit gate is transmitted to the vehicle-mounted apparatus 30 mounted on a vehicle, and for example, traffic charges or tolls corresponding to the section (route) run by the vehicle or to the type of vehicle are automatically received.

[0030]

This entrance information and exit information can be transferred by an operator via an IC card. For example, when a communication error occurs, at the recovery gate for writing in data such as the entrance information which indicates an entrance gate using the IC card or for reading out data stored in the vehicle-mounted apparatus, the IC card read/write device to which the IC card 62 can be attached and detached is used to enable execution of transfer of the entrance and exit information. Codes such as numbers or the like, which are in advance assigned respectively to positions of toll roads, may be used for the entrance information and route information.

[0031]

As shown in Fig. 3, the vehicle-mounted apparatus 30 is provided with a receiving antenna 32 for receiving a data signal transmitted from the on-road apparatus. The receiving antenna 32 is connected via a data signal receiving circuit 44 to a signal processing circuit 46 structured so as to include a microcomputer. The microcomputer of the signal processing circuit 46 stores therein a processing program, which will be described below.

[0032]

A storage circuit 48 is connected to the signal processing circuit 46. Information regarding the vehicle-mounted apparatus is stored in the storage circuit 48. Namely, when the vehicle-mounted apparatus is mounted on a vehicle, a vehicle number (the number recorded on a number plate) serving as an ID code and information regarding the type of a vehicle on which the vehicle-mounted apparatus is mounted are in advance stored in the storage circuit 48. Further, a region in which encryption information is stored is in advance allocated in the storage circuit 48. The encryption information includes the entrance information (entrance number, date and time at which the vehicle passed through the entrance gate, and the like) encrypted on a on-road apparatus side, and also includes route information regarding a check barrier (check barrier number, date and time at which the vehicle passed through the check barrier), if the vehicle passes through the mid-route (check barrier), which will be described later in detail.

[0033]

A transmission circuit 50 which transmits as a response signal a data signal including an ID code is connected to the signal processing circuit 46. The transmission circuit 50 is connected to a transmission

antenna 52. The vehicle-mounted apparatus 30 transmits the data signal from the signal processing circuit 46 via the transmission antenna 52. The transmission antenna 52 may be provided to function as a transmission/reception antenna.

[0034]

An IC card read/write device 60 is connected to the vehicle-mounted apparatus 30 so as to read data from the mounted IC card 62 and to write data in the IC card 62. The IC card read/write device 60 is equipped with a limit switch 58 which mechanically detects insertion of the IC card 62. Whether the IC card is inserted may be optically detected by determining whether light is interrupted by the inserted IC card using a photo-interrupter formed with a light emitting element and a light receiving element being disposed opposite to each other.

[0035]

Connected to the signal processing circuit 46 are a display 54 comprised of an LCD or a CRT for displaying whether the IC card is inserted or non-inserted and other information including the card value balance, and a ten-key pad 56 (a simple push-button switch may also be

used) which inputs a signal to the signal processing circuit 46.

[0036]

As shown in Fig. 4, the on-road apparatus for a vehicle traveling along the lane 202 is comprised of the mid-route antenna 218 and the mid-route antenna control device 232. The mid-route antenna 218 is comprised of a transmission antenna 22 and a receiving antenna 26. The mid-route antenna control device 232 is provided with a signal processing circuit 12 structured so as to include a microcomputer. The microcomputer stores therein a processing program which will be described later. The signal processing circuit 12 can be connected to a central computer 400 (not shown).

[0037]

The signal processing circuit 12 is connected to a transmission circuit 14 which generates a data signal including an instruction. The transmission circuit 14 is connected to the transmission antenna 22 and a signal from the transmission circuit 14 is transmitted from the transmission antenna 22. Further, connected to the signal processing circuit 12 is a receiving circuit 24 to which the receiving antenna 26 for receiving a signal

transmitted from the vehicle-mounted apparatus 30 is connected. The receiving circuit 24 fetches and outputs a data signal included in the signal transmitted from the vehicle-mounted apparatus 30, via the receiving antenna 26.

[0038]

Also connected to the signal processing circuit 12 is the memory 28. The memory 28 in advance stores therein the electronic key I. Encryption of transmitted information and decoding of received information are effected using the electronic key I in the on-road apparatus at the mid-route. The memory 28 also in advance stores therein the security mechanism A used for transfer of data between the IC card 62 and the memory 28.

[0039]

Other structures in the mid-route 200 are the same as the above-described ones, and therefore, descriptions thereof will be omitted. Further, respective antennas and antenna control devices at the entrance gate and the exit gate are substantially the same in structure as those referred to above, and descriptions thereof will be omitted.

[0040]

In the above-described vehicle-mounted apparatus and on-road apparatus, an antenna formed with a transmission antenna and a receiving antenna being separated from each other is used. However, a transmission/reception type antenna may be used.

[0041]

Further, in the above-described embodiment, the same electronic key is used both for encryption and decoding, but different electronic keys may also be used.

[0042]

As shown in Fig. 5, the IC card 62, which can be inserted in the vehicle-mounted apparatus 30, is comprised of a microcomputer including a CPU 64, a RAM 66, a ROM 68, the memory 70, and an input/output (I/O) port 72, which are connected by a bus 74 so as to allow transfer of a command or data therebetween. The memory 70 is used to store the security mechanism A and various information. The ROM 68 stores therein a processing routine which will be described later. The input/output port 72 can be connected to the vehicle-mounted apparatus 30. Although not illustrated, the IC card 62 is provided

with a power source circuit so as to supply a power source when necessary.

[0043]

The above-described IC card can store, as various information, information regarding the vehicle-mounted apparatus such as a card number, balance information, information about utilization details (entrance gate number, exit gate number, toll, time and date of utilization, and the like), and also can store a certified key code for having a card correspond to a vehicle-mounted apparatus.

[0044]

Next, an operation of the present embodiment will be described.

A description will first be given of communication processing which is mutually effected between an on-road apparatus and the vehicle-mounted apparatus. Fig. 11 shows a main process effected in each of the on-road apparatus, the vehicle-mounted apparatus, and the IC card, and a flow of information which is mutually transferred therebetween.

[0045]

As shown in Fig. 7, in step 114, the on-road apparatus located in the mid-route transmits an inquiry signal until it receives a response signal from the vehicle-mounted apparatus 30. When the on-road apparatus receives the response signal (when the decision of step 116 is affirmative), in the subsequent step 118, gate information, in this case, route information is encrypted by the electronic key I (corresponding to process S1 shown in Fig. 11). In step 120, a signal including the encrypted route information and the like is transmitted (corresponding to a transfer w1 in Fig. 11). The above-described inquiry signal includes information that indicates the kind of gate at which the on-road apparatus is provided. The information that represents the kind of gate includes, for example, a gate number expressed by a common sentence or simple common-sentence information such as "entrance", "mid-route", and the like.

[0046]

Further, in the on-road apparatus at the entrance gate, substantially the same processing as the above-described one is effected, but in place of the signal including the route information and the like, a signal including an entrance gate number indicating an

entrance gate, and the like is encrypted and transmitted. Further, in the on-road apparatus at the exit gate as well, substantially the same processing as the above-described one is effected. A toll receiving operation effected via communications will be described later.

[0047]

The on-road apparatus as can transmit, to the vehicle-mounted apparatus, simple common-sentence information as the information that indicates the kind of gate. Other information may also be selectively indicated as common-sentence information or encryption information in the on-road apparatus by separating from each other beforehand information that may be made into a common sentence as simple common-sentence information, and information that should be encrypted as encryption information.

[0048]

As described above, the on-road apparatus 10 transmits to the vehicle-mounted apparatus 30 the encryption information, and therefore, the information transferred between the on-road apparatus 10 and the vehicle-mounted apparatus 30 can maintain secrecy, and

security with respect to interception of information is improved.

[0049]

Fig. 6 shows in detail communication processing of the vehicle-mounted apparatus. When in step 102 the vehicle-mounted apparatus waits until it receives an inquiry signal from the on-road apparatus, and then receives the inquiry signal (when the decision of step 102 is affirmative), in the subsequent step 104, the vehicle-mounted apparatus reads vehicle information (for example, an ID code such as an identification code that specifies a driver's own vehicle) and transmits, as a response signal, a signal including the vehicle information.

[0050]

When in step 106 the vehicle-mounted apparatus waits until it receives a signal from the on-road apparatus and then receives the signal (when the decision of step 106 is affirmative), it is determined that certification of the on-road apparatus and the vehicle-mounted apparatus has been completed, and in the subsequent step 108, it is determined whether accounting processing is required by determining whether the kind

of gate indicates the exit gate using the information included in the inquiry signal and indicating the kind of gate at which the on-road apparatus is provided. When the kind of gate is the exit gate, accounting processing is required, and therefore, the decision of step 108 is affirmative. In step 112, the accounting processing is executed, as will be described later, and the present routine ends.

[0051]

On the other hand, when the kind of gate is an entrance gate or a mid-route, the accounting processing is not required, and therefore, the decision of step 108 is negative and the process proceeds to step 110. In step 110, information transmitted from a gate at which the accounting processing is not required, namely, encryption information based on the signal received in step 106 is stored in the storage circuit 48 as is (corresponding to a process S6 in Fig. 11) and the present routine ends. Accordingly, the contents of the entrance information or route information are stored in the storage circuit 48 of the vehicle-mounted apparatus 30 in a state of being left encrypted.

[0052]

As described above, since the entrance information or route information is maintained in the vehicle-mounted apparatus 30 in a state of being left encrypted, it becomes difficult to intercept the information transferred between the on-road apparatus 10 and the vehicle-mounted apparatus 30 resulting from a common-sentence structure and secrecy is maintained, thereby resulting in improvement of security with respect to interception of information. Further, the vehicle-mounted apparatus may merely store the encrypted information and does not need to provide a processing portion for encryption or decoding. For this reason, irregularities in charge payment caused by alteration, reproduction, and falsification due to disassembly inspection of a vehicle-mounted apparatus or analysis of a cipher are made impossible and the device configuration can be simplified.

[0053]

Next, a description will be given of processing at an exit gate.

As shown in Fig. 9, when in step 136 an on-road apparatus installed at an exit gate transmits an inquiry signal including the kind of gate until it receives a response signal from the vehicle-mounted apparatus 30 and

the on-road apparatus then receives the response signal (when the decision of step 138 is affirmative), in the subsequent step 138, the on-road apparatus transmits an information read-out requesting signal to the vehicle-mounted apparatus 30. This step 138 gives a request for reading out the encryption information stored in the storage circuit 48 of the vehicle-mounted apparatus 30 to the vehicle-mounted apparatus. Subsequently, when in step 140 the on-road apparatus transmits the information read-out requesting signal until it receives a signal from the vehicle-mounted apparatus 30 and the on-road apparatus then receives the signal (when the decision of step 142 is affirmative), in the subsequent step 144, the electronic key I is read and the received signal is decoded using the electronic key I (corresponding to a process S2 in Fig. 11).

[0054]

Meanwhile, different electronic keys I can be used at the time of encryption and decoding, and an electronic key J (≠I) used for decoding may be stored and used.

[0055]

In the subsequent step 146, using the decoded entrance information and route information and

information regarding the type of a vehicle stored in the vehicle-mounted apparatus, tolls charged the vehicle in a distance from the entrance gate, the mid-route, and until the exit gate are calculated, and data or command is generated which is used to collect automatically the calculated tolls using the IC card (corresponding to a process S3 in Fig. 11). In the subsequent step 148, the generated data or command is encrypted by the security mechanism A of the IC card (corresponding to process S4 in Fig. 11), and in the subsequent step 150, the encrypted data or command is transmitted. The data or command encrypted in step 148 is transmitted through the vehicle-mounted apparatus and is transferred to the IC card, as will be described later in detail (corresponding to a transfer w3 in Fig. 11).

[0056]

In the subsequent step 152, the on-road apparatus waits until it receives a signal from the vehicle-mounted apparatus, and when the on-road apparatus receives the signal (when the decision of step 152 is affirmative), in the subsequent step 154, the signal is decoded by the security mechanism A of the IC card. The received signal is an information signal from the IC card. In other words, the encryption information outputted from the IC card 62

is transmitted by the vehicle-mounted apparatus in a state of being left unchanged (corresponding to the transfer w3 in Fig. 11). Further, when the IC card does not have the security mechanism A, as will be described later, the IC card sends back to the on-road apparatus the encryption information in a state of being left unchanged, for example.

[0057]

In the subsequent step 154, the received signal is decoded. In step 156, based on a determination as to whether the data or command transmitted in the above-described step 150 has been sent back left unchanged, it is determined whether accounting processing has been carried out using the IC card 62 mounted on the vehicle-mounted apparatus 30. When the transmitted data or command has been sent back left unchanged, the decision of step 156 is affirmative, and in step 158, the data or command is encrypted by a security mechanism different from the security mechanism A. Thereafter, the process returns to step 150 and the above-described process is repeated.

[0058]

In the foregoing, first, a cipher is transmitted by the security mechanism A. When this mechanism is different from that at the side of the IC card 62, it is sequentially changed to the different mechanism, and thereafter, encryption is effected so as to allow coincidence of security mechanisms. Alternatively, first, the mechanism at the side of the IC card 62 is interrogated, and based on the answer thereto, the security mechanism may be determined. As a result, even when one security mechanism to be used is selected from a great number of security mechanisms, high speed processing becomes possible.

[0059]

On the other hand, when the decision of step 156 is negative, it is determined that the accounting processing has been carried out using the IC card 62. In the subsequent step 160, it is determined whether the received signal includes data indicating that reception of tolls has been completed. When the signal does not include such data, the decision of step 160 is negative and the process returns to step 152. When the received signal includes the data which indicates that reception of tolls has been completed, the decision of step 160 is affirmative. In the subsequent step 162, utilization

details regarding reception of tolls are prepared (corresponding to a process S5 in Fig. 11), and are further transmitted, together with an end signal, to the vehicle-mounted apparatus in the form of a common sentence without being encrypted (corresponding to a transfer w5 in Fig. 11). Meanwhile, the preparation of utilization details effected by the on-road apparatus and the transmission of the end signal to the vehicle-mounted apparatus may also be carried out in the IC card 62 (corresponding to a transfer w6 in Fig. 11).

[0060]

Fig. 8 shows in detail, as processing effected by the vehicle-mounted apparatus, an exit gate process in step 112 shown in Fig. 6. In step 122, the vehicle-mounted apparatus waits until it receives the information read-out requesting signal transmitted from the on-road apparatus. When the vehicle-mounted apparatus receives the information read-out requesting signal (when the decision of step 122 is affirmative), in the subsequent step 124, the encryption information stored in the storage circuit 48 is read out as is left unchanged. In the subsequent step 126, the encryption information is transmitted as is left unchanged (corresponding to a transfer w2 in Fig. 11).

[0061]

In the subsequent step 128, the vehicle-mounted apparatus waits until it receives a signal from the on-road apparatus, and when the vehicle-mounted apparatus receives the signal (when the decision of step 128 is affirmative), in the subsequent step 130, the on-road apparatus 10 and the IC card 62 are bypassed. Namely, the received signal from the on-road apparatus 10 is outputted to the IC card 62 in a state of being left unchanged, and the output signal outputted from the IC card 62 is transmitted to the on-road apparartus 10 in a state of being left unchanged (corresponding to the passing through the vehicle-mounted apparatus indicated by the transfer w3 and w4 in Fig. 11). This received signal and output signal are encrypted, and therefore, they may be temporarily stored in the vehicle-mounted apparatus.

[0062]

In the subsequent step 132, it is determined whether the received signal includes an end signal in the form of a common sentence. When the signal does not include the end signal, the decision of step 132 is negative and the process returns to step 128. When the

signal includes the end signal, the decision of step 132 is affirmative, and in step 134, bypassing of the on-road apparatus 10 and the IC card 62 is cancelled, and in the subsequent step 135, the received utilization details for reception of tolls is indicated (corresponding to a process S7 in Fig. 11).

[0063]

Fig. 10 shows a process of the IC card 62; it is determined whether a signal is inputted from the vehicle-mounted apparatus 30. When a signal is not inputted, the decision of step 164 is negative and the decision of step 164 is made repeatedly. On the other hand, when a signal is inputted (corresponding to the transfer w4 in Fig. 11), the decision of step 164 is affirmative. In the subsequent step 166, a signal inputted by decoding processing included in the security mechanism A is decoded (corresponding to a process S8 in Fig. 11). In the subsequent step 168, it is determined whether the decoded signal is a read/write request given to the IC card 62.

[0064]

When the inputted signal cannot be decoded or when a request other than the read/write request is given, the

decision of step 168 is negative. In the subsequent step 170, a signal inputted from the vehicle-mounted apparatus is sent back in a state of being left unchanged, and thereafter, the process returns to step 164. As a result, correspondence of an IC based on a plurality of different security mechanisms is made possible. On the other hand, when the process for the IC card 62 is the request for reading and writing date, the decision of step 168 is affirmative. In the subsequent step 172, it is determined whether the request is that for writing, and when the request is that for writing data, the decision of step 172 is affirmative, and the process proceeds to step 174. When the request is that for reading, the decision of step 172 is negative and the process proceeds to step 180.

[0065]

In step 174, data is written in the memory 70 by the security mechanism A. For example, reception of tolls in which tolls that are decoded data from the on-road apparatus is charged with respect to the balance of charges for accounting and the resulting balance of charges (balance information) is written in the memory 70 (corresponding to a process S9 in Fig. 11). In the subsequent step 176, the data written in the memory 70, for example, the balance information and a toll-reception

completion signal are encrypted by the securing mechanism A and are, in step 178, outputted to the vehicle-mounted apparatus 30 (corresponding to the passing through the vehicle-mounted apparatus and outputting to the on-road apparatus indicated by the transfer w4 in Fig. 11).

[0066]

In step 180, data is read from the memory 70 by the security mechanism A. In the subsequent step 182, the read data balance information, for example, is encrypted, and in step 178, it is outputted to the vehicle-mounted apparatus 30.

[0067]

As described above, in the present embodiment, among information to be communicated between the on-road apparatus and the vehicle-mounted apparatus, information such as entrance information or route information, which has a high secrecy to prohibit alteration thereof, is used in a state of being left encrypted (in the form of encryption information) and the encrypted information is temporarily stored in the vehicle-mounted apparatus as it is. Accordingly, alteration of information such as entrance information or route information becomes difficult; therefore, the reliability of the information

itself can be improved and the secrecy thereof can be maintained.

[0068]

Further, in a case in which reading and writing is effected for an IC card in which user information regarding a user such as the balance of charges or the like is stored, when information is transferred using the encryption information encrypted by the security mechanism of the IC card itself and the information of the IC card is outputted via the vehicle-mounted apparatus which transmits and receives information to and from the on-road apparatus, or when the information from the on-road apparatus is inputted, the vehicle-mounted apparatus merely allows passing of the encrypted information and does not decode the information. Accordingly, information is not altered and the secrecy thereof can be maintained.

[0069]

Moreover, the vehicle-mounted apparatus merely allows passing of the encryption information therethrough, and therefore, the vehicle-mounted apparatus does not need to provide processing for encryption or decoding. As a result, the structure of

the vehicle-mounted apparatus is simplified and a calculation load of the vehicle-mounted apparatus can be reduced.

[0070]

Further, in the road-to-vehicle communications, a two-way communication (optical communication or the like is also possible) is employed and the present invention can be applied thereto.

[0071]

The above-described system can be applied to a road or a parking area for simple reception of tolls wherein a gate is not present.

[0072]

Further, in the above-described system, there was described a case in which a vehicle-mounted apparatus includes neither a structure nor a process for encryption and decoding, but a common sentence-structured portion may be deleted by well-known general encryption.

[0073]

[Effects of the Invention]

The vehicle-mounted communication device of the present invention has an effect in that, among the information received from the road side by the transmitting/receiving means, the encryption information is relayed to the IC card by the relay means. Accordingly, the encryption information passes through the vehicle-mounted communication device in a form of being left unchanged, and thus, the secrecy of the encryption information is maintained and the security thereof is protected.

[0074]

The road-to-vehicle communication device of the present invention has an effect in that, the IC card is mounted in the vehicle-mounted communication device that relays encryption information, and information is mutually communicated with respect to the road-side control means that encrypts transmitted information and decodes received information. Accordingly, the secrecy of the information is maintained and the security thereof is protected.

[BRIEF DESCRIPTION OF THE DRAWINGS]

[Fig. 1]

Fig. 1 is a block diagram that shows an automatic toll receiving system to which the present invention is applicable.

[Fig. 2]

Fig. 2 is a schematic perspective view that shows a mid-route in the automatic toll receiving system.

[Fig. 3]

Fig. 3 is a block diagram that shows a vehicle-mounted apparatus of the present embodiment.

[Fig. 4]

Fig. 4 is a block diagram that shows one example of an on-road apparatus of the present embodiment.

[Fig. 5]

Fig. 5 is a block diagram that shows a structure of an IC card to which the present invention is applicable.

[Fig. 6]

Fig. 6 is a flow chart that shows a flow in a process of the vehicle-mounted apparatus.

[Fig. 7]

Fig. 7 is a flow chart that shows a flow in a process of the on-road apparatus in a mid-route.

[Fig. 8]

Fig. 8 is a flow chart that shows a flow in an exit gate process of the vehicle-mounted apparatus.

[Fig. 9]

Fig. 9 is a flow chart that shows a flow in a process of the on-road apparatus at an exit gate.

[Fig. 10]

Fig. 10 is a flow chart that shows a flow in a process of the IC card.

[Fig. 11]

Fig. 11 is an image diagram that shows the relationship between the on-road apparatus, the vehicle-mounted apparatus, and the IC card when information is mutually transferred therebetween.

[Description of the Reference Numerals]

10: on-road apparatus

28: memory

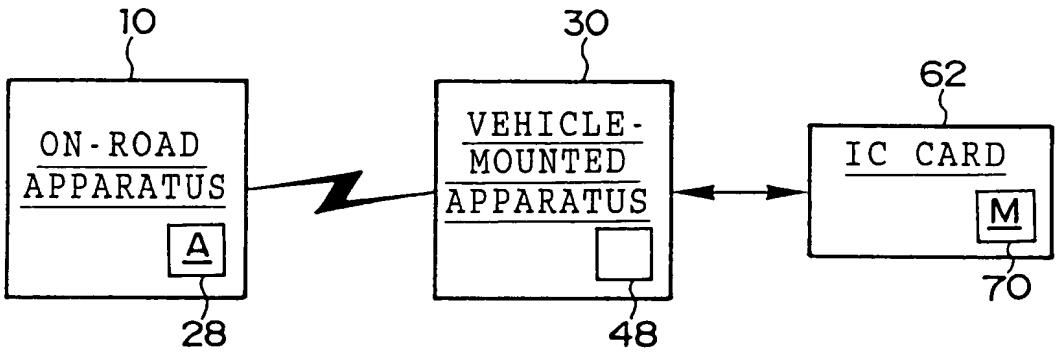
30: vehicle-mounted apparatus

48: storage circuit

62: IC card

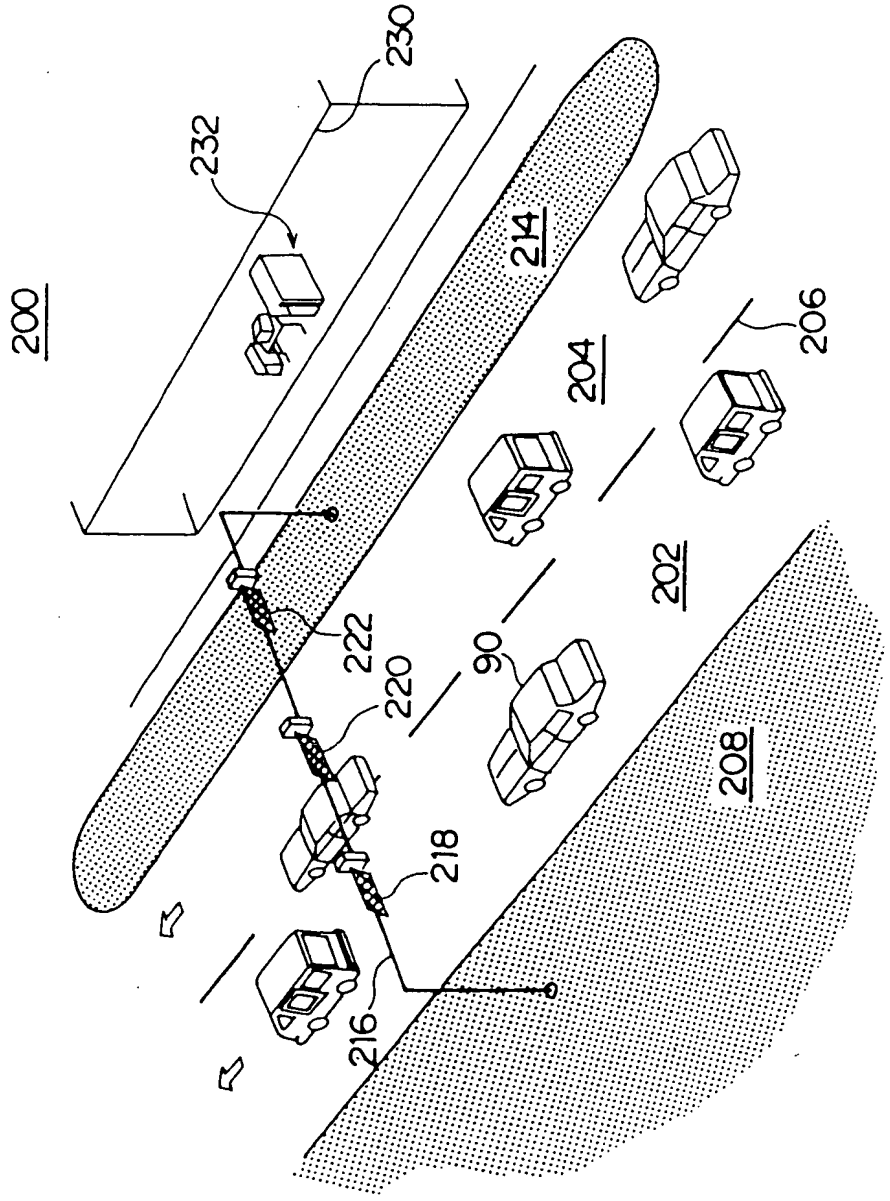
70: memory

[DOCUMENT NAME] DRAWINGS
[FIG. 1]

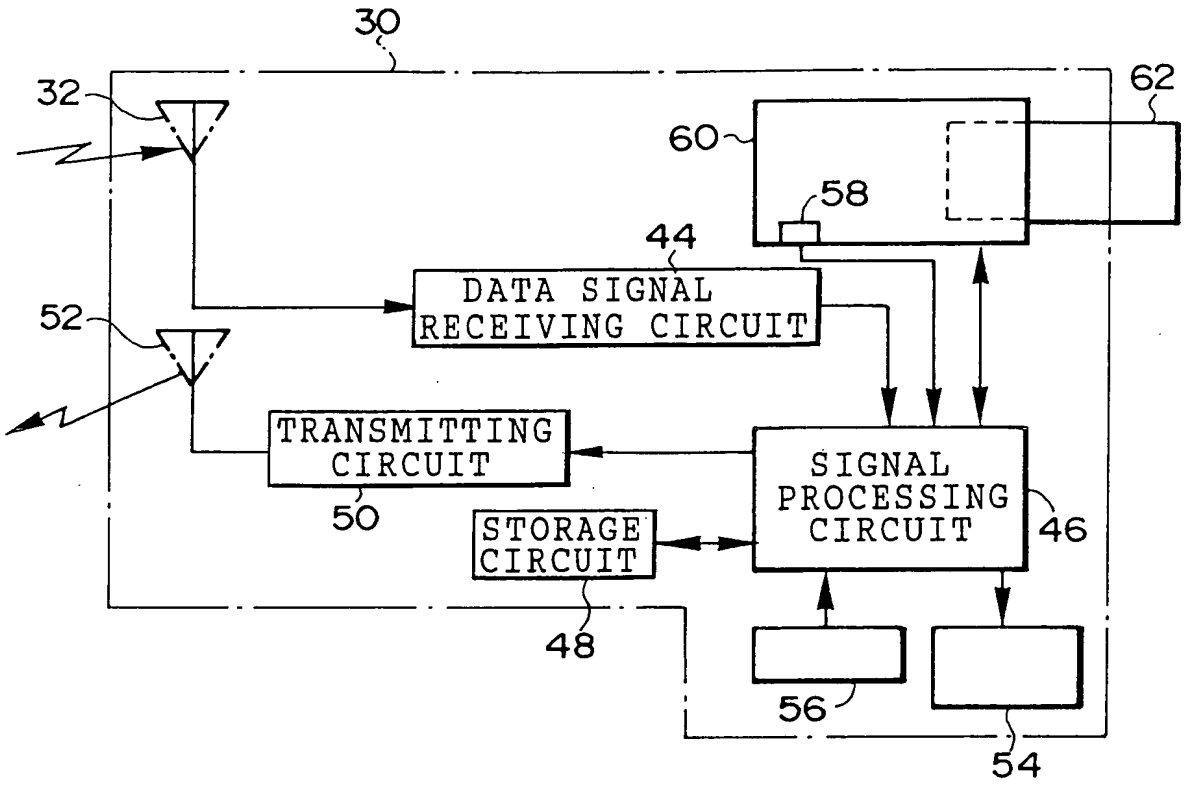


10: ON-ROAD APPARATUS
28: MEMORY
30: VEHICLE-MOUNTED APPARATUS
48: STORAGE CIRCUIT
62: IC CARD
70: MEMORY

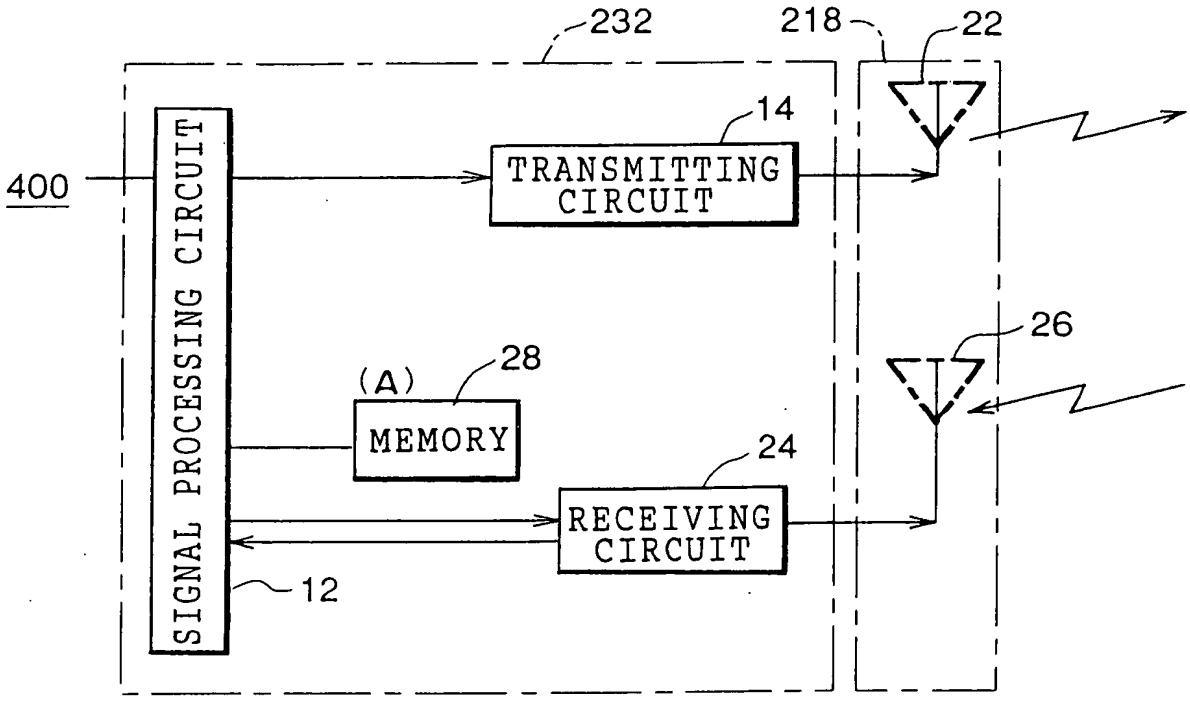
[FIG. 2]



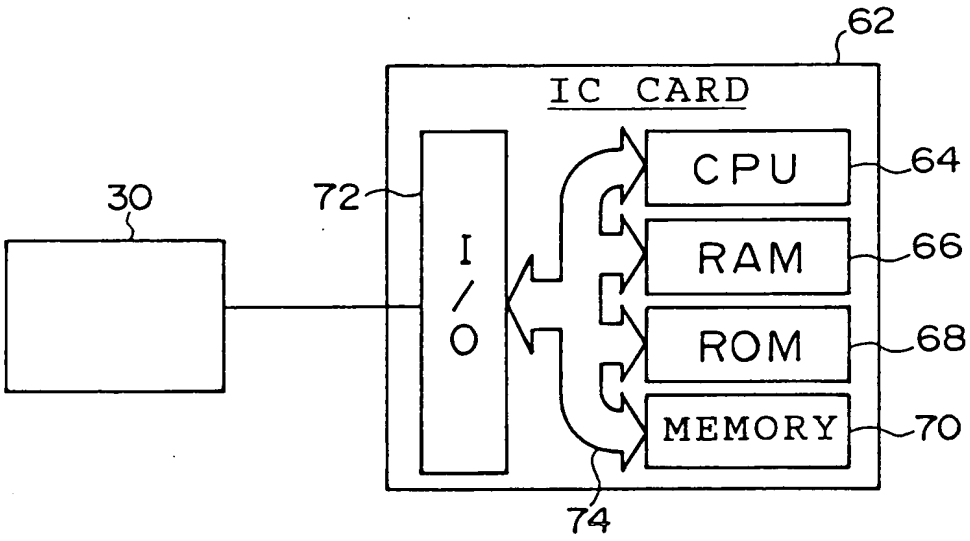
[FIG. 3]


30
32
62
60
58
44
DATA SIGNAL RECEIVING CIRCUIT
52
TRANSMITTING CIRCUIT
50
SIGNAL PROCESSING CIRCUIT
46
STORAGE CIRCUIT
48
56
54

[FIG. 4]

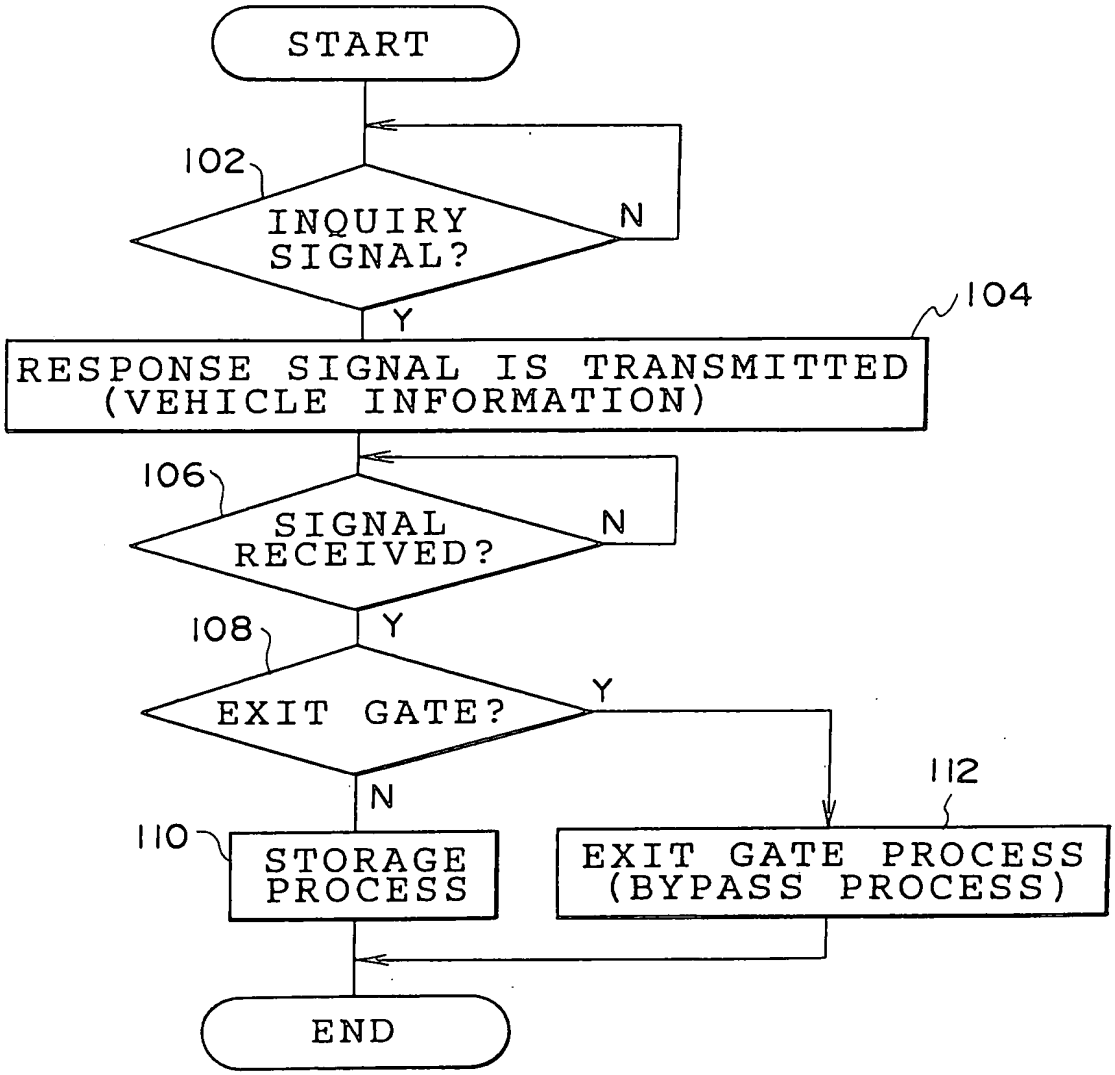

232
218
22
14
400
TRANSMITTING CIRCUIT
SIGNAL PROCESSING CIRCUIT
26
(A)
28
MEMORY
24
RECEIVING CIRCUIT
12

[FIG. 5]



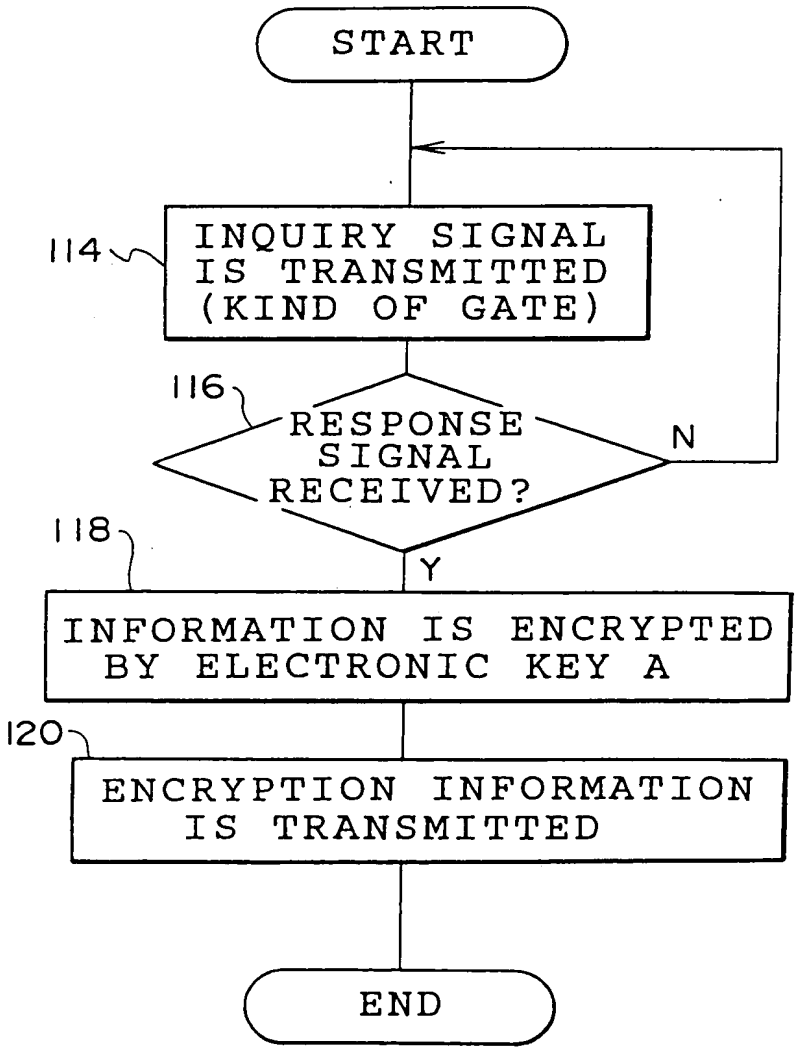
[FIG. 6]

PROCESS OF VEHICLE-MOUNTED APPARATUS



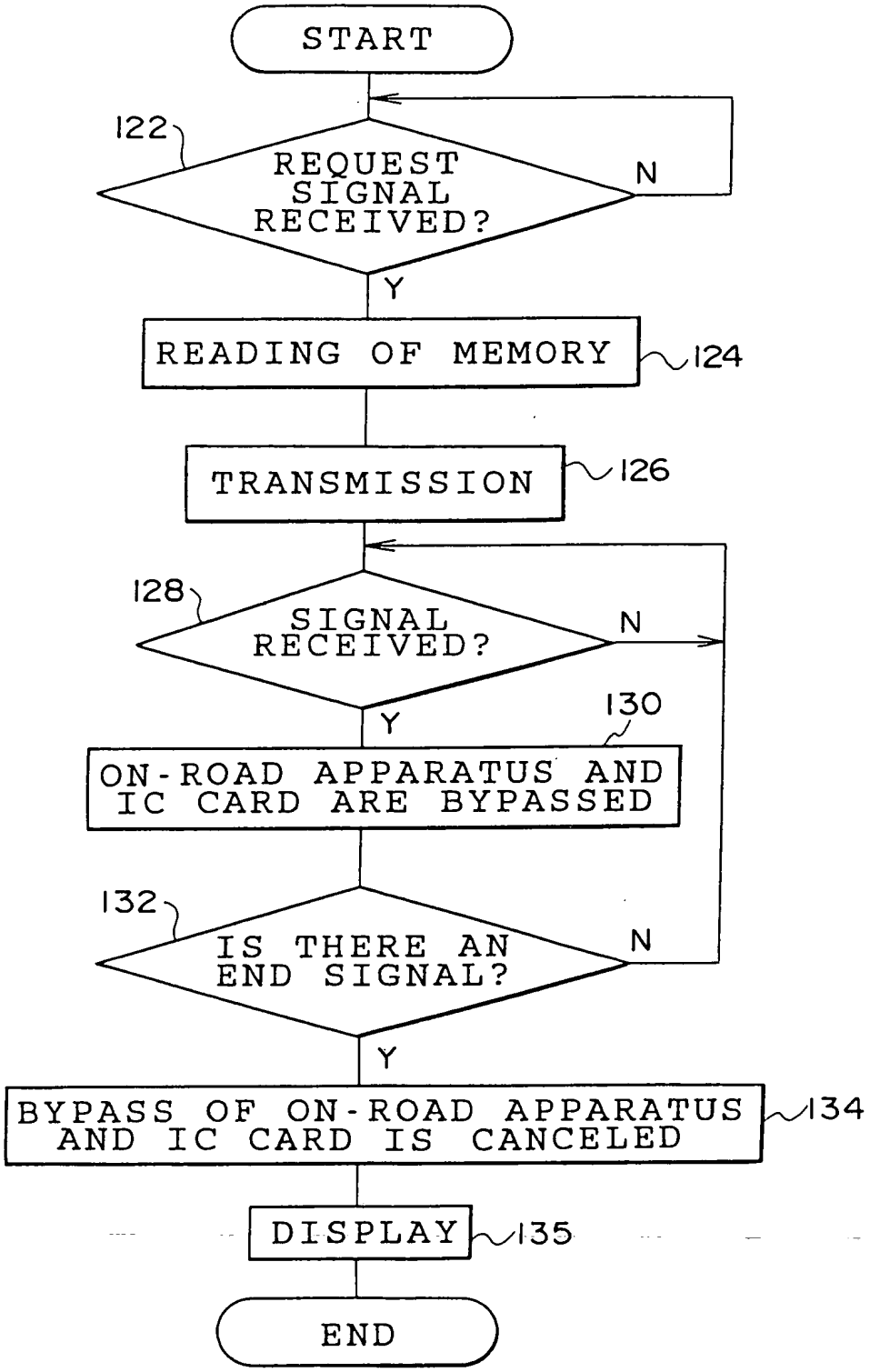
[FIG. 7]

PROCESS OF ON-ROAD APPARATUS



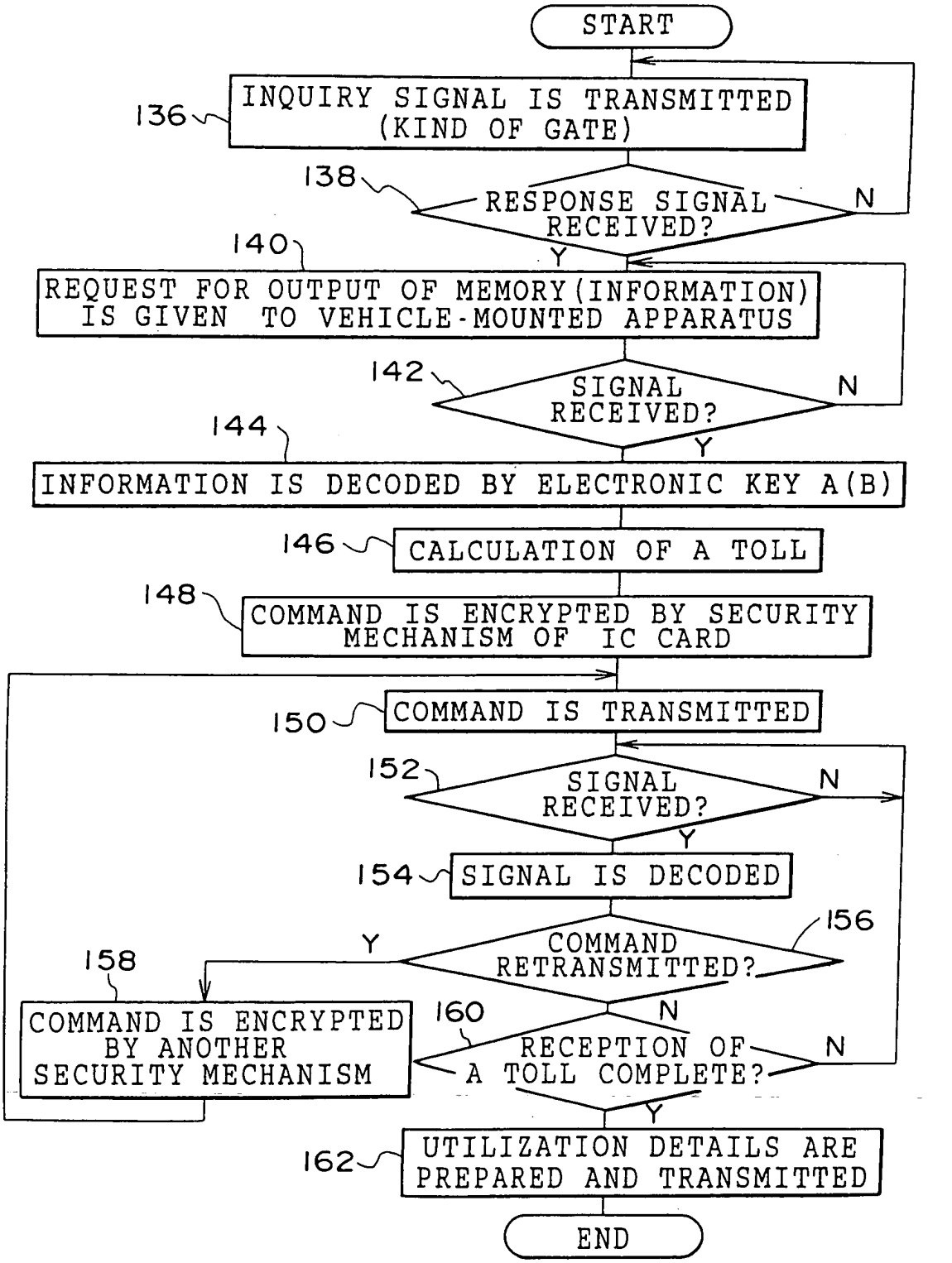
[FIG. 8]

EXIT GATE PROCESS OF VEHICLE-MOUNTED APPARATUS

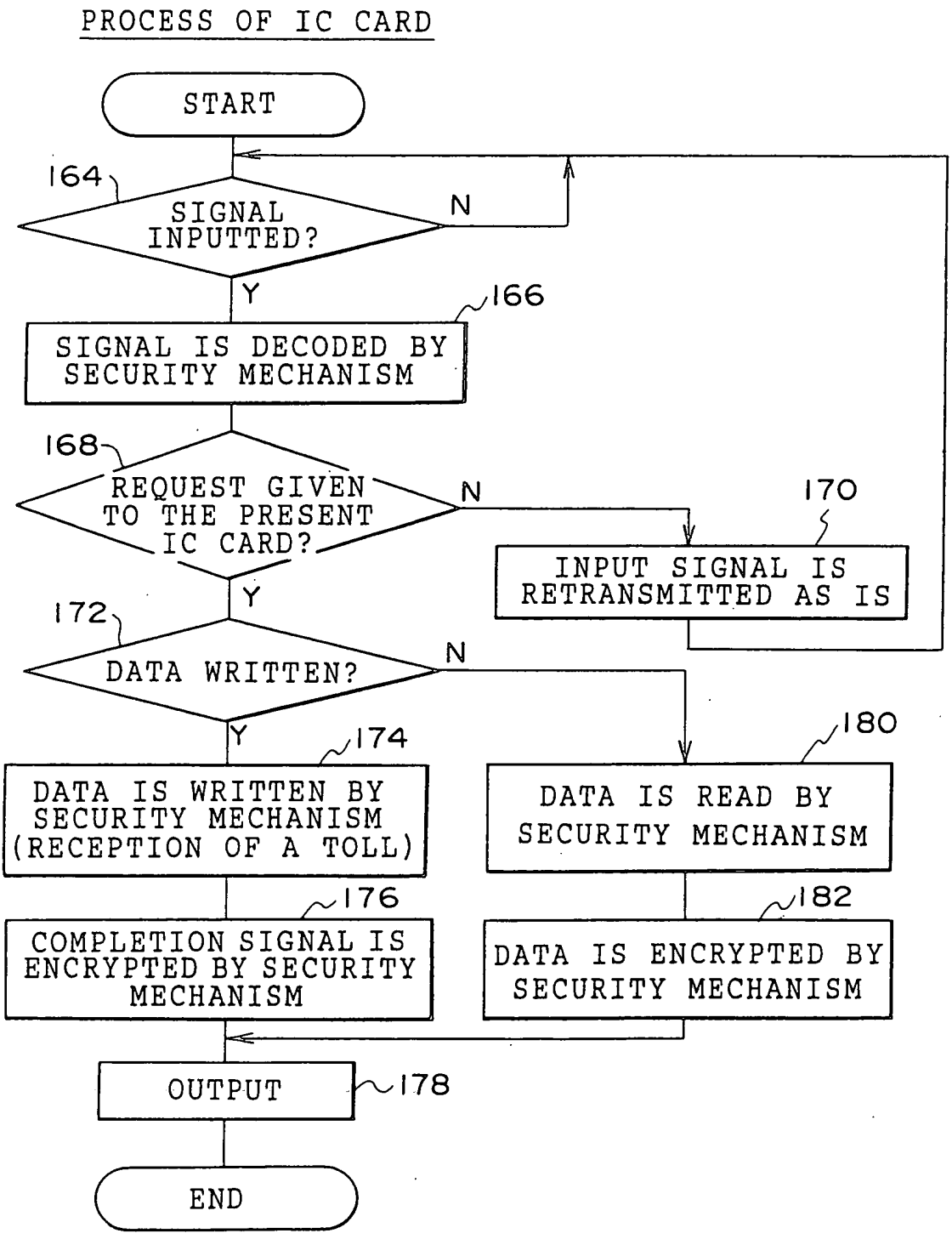


[FIG. 9]

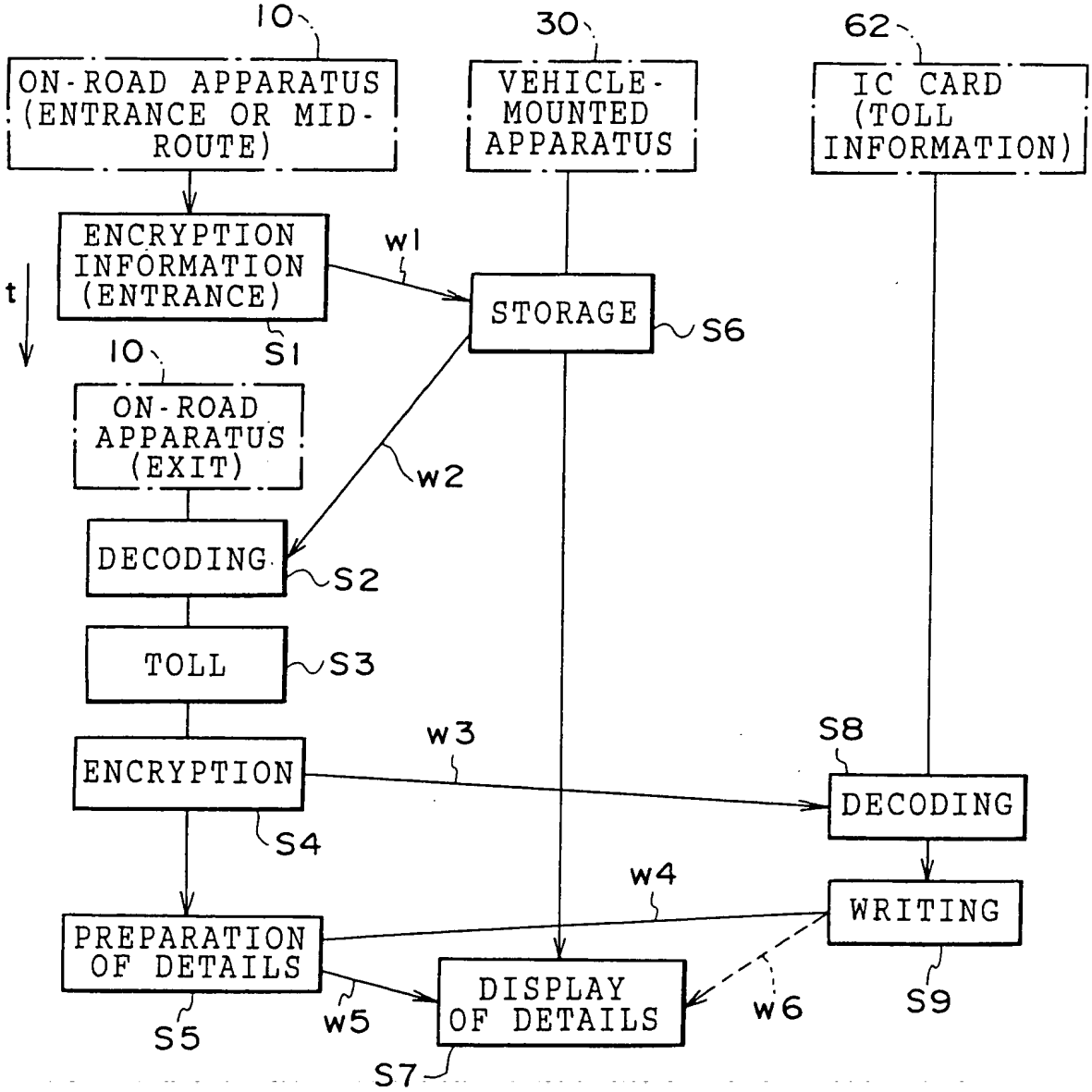
PROCESS OF ON-ROAD APPARATUS AT EXIT GATE



[FIG. 10]


PROCESS OF IC CARD
START
164
SIGNAL INPUTTED?
N
Y
166
SIGNAL IS DECODED BY SECURITY MECHANISM
168
REQUEST GIVEN TO THE PRESENT IC CARD?
N
170
INPUT SIGNAL IS RETRANSMITTED AS IS
Y
172
DATA WRITTEN?
N
Y
174
DATA IS WRITTEN BY SECURITY MECHANISM (RECEPTION OF A TOLL)
180
DATA IS READ BY SECURITY MECHANISM
176
COMPLETION SIGNAL IS ENCRYPTED BY SECURITY MECHANISM
182
DATA IS ENCRYPTED BY SECURITY MECHANISM
OUTPUT
178
END

[FIG. 11]


10
30
62
ON-ROAD APPARATUS (ENTRANCE OR MID-ROUTE)
VEHICLE-MOUNTED APPARATUS
IC CARD (TOLL INFORMATION)
ENCRYPTION INFORMATION (ENTRANCE)
w1
STORAGE
S6
t
S1
10
ON-ROAD APPARATUS (EXIT)
w2
DECODING
S2
TOLL
S3
ENCRYPTION
w3
S8
DECODING
S4
w4
WRITING
PREPARATION OF DETAILS
DISPLAY OF DETAILS
w6
S9
S5
w5
S7

[DOCUMENT NAME] ABSTRACT OF THE DISCLOSURE

[SUMMARY]

[OBJECT]

To provide a vehicle-mounted communication device and a road-to-vehicle communication device which each allow communication of information using a simple structure by making leakage of information difficult.

[MEANS FOR SOLUTION]

Information including encryption information is communicated between an on-road apparatus 10 having a memory 28 in which an electronic key I is stored, and a vehicle-mounted apparatus 30 having a storage circuit 48. Encrypted route information and the like are stored as is in the vehicle-mounted apparatus 30. Encryption and decoding are executed at an on-road apparatus side. In reception of charges, encrypted information from an IC card 62 having a memory 70 in which a security mechanism is stored passes through the vehicle-mounted apparatus and is transferred to the on-road apparatus. The encrypted information from the IC card 62 is decoded with the on-road apparatus. Accordingly, the encrypted information is mutually transferred between these apparatuses and the vehicle-mounted apparatus does not require encryption or decoding. As a result, the security of a system can be improved.